论文

基于网络编码的匿名通信模型

周彦伟^{①②}, 杨波^{②*}, 吴振强^{①②}, 何聚厚^{①②}, 李骏^①

① 现代教学技术教育部重点实验室 (陕西师范大学), 西安 710062

② 陕西师范大学计算机科学学院, 西安 710062

* 通信作者. E-mail: byang@snnu.edu.cn

收稿日期: 2013-10-29; 接受日期: 2013-12-11

国家自然科学基金 (批准号: 61173190, 61272436)、广东省自然科学基金 (批准号: 10351806001000000) 和陕西省自然科学基金基础研究计划 (批准号: 2012JQ8023) 资助项目

摘要 网络编码技术的提出彻底改变传统网络的传输方式, 本文基于信息分割理论和网络编码技术提出一种新型的匿名通信模型 (anonymous communication model based on network coding, ACM-NC), 信息分割技术将匿名通信消息分割后经不同的匿名链路进行编码传输; 转发网络节点的编码传输机制在提高系统匿名性、安全性和保密性的同时增强了抗合谋攻击的能力. 理论分析及仿真结果表明, ACM-NC 具有较强的匿名性、安全性、保密性和抗合谋攻击的能力, 并且 ACM-NC 中仅有信宿节点才能通过解码编码消息恢复信源节点的原始匿名通信消息.

关键词 信息分割 匿名通信 网络编码 合谋攻击 网络安全

1 引言

匿名通信就是在不改变现有网络协议的前提下, 实现对通信过程中通信关系及个人隐私信息的保护, 使窃听者无法直接获知或间接推知双方的通信关系或身份. 匿名通信系统指保护用户间通信关系和用户身份、行为和位置等个人隐私信息的通信模型, 其往往通过加密、代理、混淆和广播等技术将通信关系或通信消息进行隐藏, 使得攻击者和窃听者都无法识别出通信消息和通信双方间的关系, 更无法获知通信双方的身份、行为和位置等个人隐私信息. 然而传统匿名通信系统一般基于可信密钥分发中心进行事先分发密钥或相关参数, 或者基于密钥基础设施进行会话密钥的协商, 所以传统匿名通信系统的安全性及通信消息的保密性完全依赖于密钥的安全性, 系统中必须有可信第三方参与会话密钥的协商或者事先分发密钥等, 这将导致密钥管理的复杂化, 也增加了匿名通信系统的实施代价; 同时, 也造成传统匿名通信系统在分布式网络环境 (如 P2P 网络) 下由于无信任中心而无法部署. 因此, 研究无可信密钥分发中心环境下的匿名通信机制已成为当前匿名通信领域的热点研究问题.

鉴于传统匿名通信系统存在的上述问题, 针对无可信密钥分发中心的网络环境, 本文提出基于网络编码的匿名通信模型 (anonymous communication model based on network coding, ACM-NC). ACM-NC 中信源节点使用若干可信节点建立发送匿名组和接收匿名组, 同时选择若干节点构造编码匿名转发网络; 信源节点根据信息分割策略将通信消息分割成分片消息, 产生随机编码系数对分片消息进行编码操作; 同时将编码分片消息和随机编码系数的按位等分分量一起分别沿不同的匿名链路传输; 编

引用格式: 周彦伟, 杨波, 吴振强, 等. 基于网络编码的匿名通信模型. 中国科学: 信息科学, 2014, 44: 1560–1579, doi: 10.1360/N112013-00154

码匿名转发网络中各节点选择随机编码系数对其所接收的消息进行编码转发, 同时将随机编码系数分量分散到不同的匿名链路进行传输; 最后, 所有的编码消息片和随机编码系数分量在信宿节点会合, 由信宿节点还原出信源节点的原始通信消息.

本文的结构安排为: 第 2 节介绍相关研究工作; 第 3 节提出基于网络编码的匿名通信模型 ACM-NC, 并对 ACM-NC 的具体工作过程及相关关键技术进行详细介绍; 第 4 节对 ACM-NC 的匿名性、安全性和保密性进行分析; 最后是总结与展望.

2 相关工作

2.1 匿名通信机制

传统匿名通信系统一般是基于密钥基础设施, 即系统存在可信的密钥分发中心为各节点事先分配密钥或相关参数, 各节点基于已有的公钥或共享密钥传输匿名链路的建立信息. 常见的匿名通信协议和系统原型主要有 Onion Routing, Tor, Mix, Crowds, DC-Net, Sherwood 和 Tarzan 等, 其主要的工作原理及不足如下所述.

洋葱路由 (onion routing)^[1] 是利用公钥嵌套加密机制, 将下一跳的地址封装在节点的加密结构中, 使得路径上任意节点仅能获知下一跳的地址, 而无法解密其他节点的路径信息. 但该机制以公钥为基础实现匿名通信, 增加了系统的复杂性, 同时公钥加密的计算代价较大, 会导致通信时延的增加.

针对公钥加密代价大的问题, 第二代洋葱路由 (the second-generation onion routing, Tor)^[2] 使用了 Diffie-Hellman 密钥协商协议完成信源节点与路径各节点的密钥协商, 并基于协商密钥加密传输包含下一跳节点的建路信息, 但该机制需要可信的第三方来管理密钥参数的分配和更新, 不可避免地增加了密钥管理开销, 因此其通信时延和计算复杂度依然较大.

混淆模型^[3] 通过多个混淆器对数据转发实现匿名的过程. 该模型由于插入随机时延和消息, 导致其计算开销大、网络拥塞频繁, 并且通信延迟较大, 这些缺点已严重影响其推广应用.

Crowds^[4] 系统采用下一跳路由方式, 路径上的任意节点均掌握目标节点的相关信息. 该机制建路过程无需密钥参与, 而是由中间节点以一定概率来选择传输给下一跳节点还是传输给接收者, 但 Crowds 仍需可靠、可信的密钥分发中心来分配通信密钥, 同时 Crowds 无法实现接收者匿名.

文献 [5] 指出在 DC-Net^[6], Sherwood^[7] 和 Tarzan^[8] 等匿名通信系统中普遍存在传输代价大的缺点.

传统匿名通信系统基于密码基础设施的方法具有很好的信息保密性, 但密钥的事先分发及协商将增加密钥管理的复杂性和部署代价, 同时节点的加解密机制使得传输网络的计算负载较重. 因此, 研究无可信密钥分发中心环境下的匿名通信机制具有重要的研究意义.

2.2 信息分割策略

在文献 [9,10] 中提出利用信息分割传输的方式将信息分割后沿着不相交的路径发送给链路上的每一个节点. 文献 [5] 将该方法称为源信息分割策略 (source information slicing, SIS), 该策略为无密钥基础设施环境下匿名传输路径的建立奠定了基础. 但是, 只要转发网络每条转发链路的任意位置存在一个泄密节点, 泄密节点通过合谋就可以恢复出相应的信息内容, 因此信息分割策略使用在通信过程时, 需要对通信消息进行相应的处理, 增加泄密节点合谋还原原始通信消息的复杂性.

文献 [5] 基于信息分割传输策略提出了一种无需密钥基础设施的匿名通信机制 AC-ITNC, 该机制将建路信息分割后编码传送, 实现无可信密钥分发中心环境下节点间会话密钥的安全协商及匿名通信链路的安全建立, 分析表明 AC-ITNC 显著提高了匿名通信系统建路阶段的抗合谋攻击能力, 为无可信中心环境下匿名通信机制的研究提出新的研究思路; 但该机制在匿名通信阶段未使用相关分割传输策略, 也未使用编码技术处理原始匿名通信消息, 而是采用传统的匿名通信方式进行信源节点与信宿节点间的匿名通信, 因此在 AC-ITNC^[5] 中转发匿名链路的首、尾节点必须为可信节点, 否则首尾节点将泄漏信源节点和信宿节点的身份、行为和位置等隐私信息, 并且 AC-ITNC 是基于协商密钥的安全性构建其安全性。

2.3 网络编码

2000 年, Ahlswede 等^[11] 以著名的“蝴蝶网络”模型为例阐述了网络编码的基本原理。由于网络编码技术的提出彻底改变了传统网络的传输模型, 因此该技术已成为当前信息传输领域的研究热点, 众多学者在网络编码的分类、构造算法、优化和应用等方面进行了大量研究^[12~20]:

(1) 网络编码的分类

根据网络节点对传输信息是否进行线性操作, 可将网络编码分为线性网络编码^[12] 和非线性网络编码; 根据网络节点的信息操作系数是否随机选取, 可将网络编码分为随机网络编码^[13] 和确定性网络编码。

(2) 网络编码构造算法

文献 [12,14,15] 详细介绍了指数时间算法^[14]、多项式时间算法^[15] 和贪婪算法^[12] 这三种典型的网络编码构建算法, 由于多项式时间算法具有较低的复杂性, 具有重要的理论研究意义和应用推广价值。

(3) 网络编码优化

文献 [16] 分析认为影响网络编码实现复杂性的主要因素有: 编码构造算法、编码操作数以及有限域的大小等; 文献 [17] 基于将普通网络转化为某种易于表达且各网络节点具有共同特征的“简单网络”的思想, 提出了一种基于简单网络的最小代价编码方案; 文献 [18] 基于信息流分解方案对网络编码进行优化, 提出基于信息流分解的网络编码优化模型。

(4) 网络编码的应用

文献 [19] 提出了第一个实用的网络编码方案, 由各节点分布式随机产生编码系数, 再将编码系数矩阵携带在数据包中进行传输, 信宿节点依据接收到的编码数据包, 通过解码获得信源节点的通信消息, 增强了消息传输过程的安全性, 同时使得网络编码技术的发展具有了质的飞跃; 文献 [20] 基于网络编码技术对无线传输技术进行了研究; 文献 [21~23] 等对网络编码在无线自组织网络^[21]、无线传感器网络^[22] 和无线网状网^[23] 中的应用进行了探讨。

3 基于网络编码的匿名通信模型

传统通信网络中, 节点仅具有数据转发的功能, 网络编码技术的提出彻底改变了传统通信网络的消息转发策略, 在网络编码环境中, 转发网络的各中间节点能够对其所接收的通信消息进行编码转发。如图 1 所示, 受文献 [5] 的启发本文提出了一种基于网络编码的匿名通信模型——ACM-NC, 在匿名

图 1 基于网络编码的匿名通信模型

Figure 1 Anonymous communication model based on network coding

通信阶段使用信息分割技术和编码传输策略, 舍弃传统匿名通信系统的密钥协商过程, 在无密钥分发中心环境下构建匿名通信机制, 增强匿名通信系统消息传输阶段的安全性、匿名性及抗合谋攻击性。

(1) 本文使用的相关定义表述如下:

定义 1 $\bigoplus_{i=1}^n X_i$ 表示 n 个数据 $x_1, x_2, \dots, x_n$ 进行异或运算, 即 $\bigoplus_{i=1}^n X_i = x_1 \oplus x_2 \oplus \dots \oplus x_n$.

定义 2 $x_1 || x_2$ 为拼接运算, 即将数据 x_1 和 x_2 的二进制位串进行连接运算, 拼接运算过程中以 x_1 作为高位, x_2 作为低位形成一个新的二进制数据。

定义 3 $\bigparallel_{i=1}^n X_i$ 表示 n 个数据 $x_1, x_2, \dots, x_n$ 进行拼接运算, 即 $\bigparallel_{i=1}^n X_i = x_1 || x_2 || \dots || x_n$.

定义 4 $C \oplus V$ 表示向量 C 与向量 V 的异或运算, 即向量 C 和 V 的相关元素进行异或运算后组成的向量。

定义 5 $C || V$ 表示向量 C 与向量 V 的拼接运算, 即向量 C 和 V 的相关元素进行拼接运算后组成的向量。

定义 6 函数 $f(x)$ 为消息分割函数, 该函数可将消息 M 分割成 m 份分片消息 $M_1, M_2, \dots, M_m$, 并且 $f(x)$ 是可逆函数, 即存在逆函数 $f^{-1}(x)$, 可通过 $f^{-1}(x)$ 依据分片消息能够还原出原始通信消息。消息分割函数 $f(x)$ 的具体构造非本文的研究重点, 文献 [9,10] 对信息分割理论进行了详细介绍, 本文不再赘述。

定义 7 $E(k, M)$ 和 $D(k, C)$ 表示对称密钥加密/解密算法。

(2) 本文使用的相关变量及符号定义如下:

$O_{(i,j)} (i = 1, 2, \dots, m, j = 1, 2, \dots, n)$ 表示编码匿名转发网络的中继节点, 即为第 i 条匿名通信链路的第 j 个节点。

$M_{(i,j)}$ 表示节点 $O_{(i,j)}$ 使用随机编码系数编码后的编码消息块, 即分片消息 M_i 先后分别经过信源节点和节点 $O_{(i,1)}, O_{(i,2)}, \dots, O_{(i,j)}$ 编码后的编码消息。

$V_{(i,j)}$ 表示节点 $O_{(i,j)}$ 计算得到的随机编码系数分量的累积异或向量, 即转发网络中前 $(j-1)$ 列的 $m(j-1)$ 个节点随机编码系数的第 i 个分量与信源节点随机编码系数的第 i 个分量进行异或运算得到的累积异或向量, 称向量 $V_{(i,j)}$ 为消息还原向量。

$C_{(i,j)}$ 表示节点 $O_{(i,j)}$ 选择的长度为 L 随机编码系数。

$C_{(i,j)}^N (N = 1, 2, \dots, m)$ 表示节点 $O_{(i,j)}$ 随机编码系数 $C_{(i,j)}$ 的分量, 即 $C_{(i,j)}$ 按二进制位等分成 m 个分量, $C_{(i,j)}^N$ 表示其中的第 N 个分量, 在转发网络中沿第 N 条匿名链路进行传输.

$Z_{O(i,j)}$ 表示节点 $O_{(i,j)}$ 接收到前驱节点 $O_{(i,j-1)}$ 的随机编码系数分量所组成的向量, 即 $Z_{O(i,j)} = (C_{(1,j-1)}^i, C_{(2,j-1)}^i, \dots, C_{(m,j-1)}^i)$.

M_{Bob} 表示由信宿节点 Bob 接收到编码匿名转发网络发送的所有编码分片消息所组成的向量, 即 $M_{\text{Bob}} = (M_{(1,n)}, M_{(2,n)}, \dots, M_{(m,n)})$.

M_{Alice} 表示由信源节点 Alice 产生的编码分片消息组成的向量, 即 $M_{\text{Alice}} = (M_{(1,0)}, M_{(2,0)}, \dots, M_{(m,0)})$.

(3) 本文相关假设条件表述如下:

本文 ACM-NC 的安全性将基于下述假设实现.

假设 编码匿名转发网络出现网络差错的概率可忽略, 即信宿节点能够完全接收信源节点发送的编码分片消息及转发网络中各节点产生的随机编码系数.

3.1 编码匿名转发网络

本文借鉴文献 [5] 密钥协商机制的相关理论和文献 [9] 信息分割策略完成匿名转发网络的建立. 如图 1 所示信源节点 (即发送者) 为 Alice, 信宿节点 (即接收者) 为 Bob. Alice 选择 $m \times n$ 个节点, 建立 m 条长度为 n 的匿名通信链路 (简称: 匿名链路), 将由 $m \times n$ 个节点及各节点间的通信链路组成的网络称为编码匿名转发网络 (简称: 转发网络), 即转发网络由 m 条长度为 n 的匿名链路组成, 则 $O_{(i,j)} (i=1, 2, \dots, m; j=1, 2, \dots, n)$ 是第 i 条链路上的第 j 个节点. 转发网络建立过程中 Alice 将转发网络中各节点所有后继节点的 IP 地址分别发给对应的节点, 协助各节点建立通信路由表, 即在无代理和可信密钥分发中心的网络环境中建立了匿名通信链路, 并且确保转发网络中各节点仅知晓其前驱节点和后继节点, 即节点 $O_{(i,j)}$ 的前驱节点为 $O_{(k,j-1)} (k=1, 2, \dots, m)$, 当 $k=i$ 时称节点 $O_{(k,j-1)}$ 是 $O_{(i,j)}$ 的直接前驱节点; 节点 $O_{(i,j)}$ 的后继节点则是 $O_{(k,j+1)}$, 当 $k=i$ 时称节点 $O_{(k,j+1)}$ 是 $O_{(i,j)}$ 的直接后继节点, 则在转发网络中, 每个节点有 m 个前驱节点的同时有 m 个后继节点.

Alice 首先将消息 Message 分割成分片消息 $M_1, M_2, \dots, M_m$, 并产生随机编码系数 $C_{(i,0)} (i=1, 2, \dots, m)$ 对分片消息进行编码操作, 并将 $C_{(i,0)}$ 按二进制位等分成 m 个分量 $C_{(i,0)}^N (N=1, 2, \dots, m)$. 然后 Alice 从本区域选择一定数量的可信节点组成发送匿名组, 在发送匿名组中, Alice 基于改进的 ECDH 算法 [24] 与各节点间协商安全的会话密钥. 最后 Alice 使用可信节点建立发送匿名链路, 并按匿名链路中可信节点的顺序从后至前嵌套加密形成洋葱型通信数据包. 在发送匿名组中, 封装数据每经过一个节点被解密一层, 直至出口节点时, 嵌套加密消息被完全解密, 出口节点再将 $M_{(i,0)}$ 和 $V_{(i,0)}$ 通过转发网络中的第 i 条链路发送.

匿名链路中任意节点 $O_{(i,j)}$ 选择随机编码系数 $C_{(i,j)}$ 对收到的编码消息 $M_{(i,j-1)}$ 进行编码, 将编码后的编码消息 $M_{(i,j)}$ 发给 $O_{(i,j+1)}$, 将随机编码系数等分成 m 个分量后沿 m 条不同的匿名链路传递至节点 $O_{(a,j+1)} (a=1, 2, \dots, m)$.

同理, Alice 选择可信节点组成接收匿名组, 转发网络中各匿名链路的第 n 个节点 $O_{(i,n)}$ 将其所接收的消息以广播通信方式发送给接收匿名组中的每个成员, 但仅有信宿节点才能还原信源节点的原始通信消息.

3.2 信源节点的信息分割和编码策略

Alice 通过消息分割函数 $f(M, m)$ 将原始通信消息 Message 分割成 m 份长度为 L 的分片消息 $M_1, M_2, \dots, M_m$. 同时, Alice 随机选取 m 个长度为 L 的编码系数 $C_{(i,0)}$ 分别对分割后的分片消息 M_i 按式 (1) 进行异或编码运算.

$$M_{(i,0)} = C_{(i,0)} \oplus M_i (i = 1, 2, \dots, m). \quad (1)$$

Alice 将编码系数 $C_{(i,0)}$ 按二进制位等分成 m 个编码系数分量 $C_{(i,0)}^1, C_{(i,0)}^2, \dots, C_{(i,0)}^m$; 即 $C_{(i,0)} = \bigvee_{k=1}^m C_{(i,0)}^k$, 最后一个编码系数分量 $C_{(i,0)}^m$ 的长度为 $L - (m-1) \lfloor \frac{L}{m} \rfloor$, 而其他各编码系数分量的长度均为 $\lfloor \frac{L}{m} \rfloor$.

Alice 对分片消息 $M_1, M_2, \dots, M_m$ 进行编码处理, 则编码消息向量 M_{Alice} 为

$$M_{\text{Alice}} = (M_{(1,0)} = C_{(1,0)} \oplus M_1 = \bigvee_{i=1}^m C_{(1,0)}^i \oplus M_1, \\ M_{(2,0)} = C_{(2,0)} \oplus M_2 = \bigvee_{i=1}^m C_{(2,0)}^i \oplus M_2, \dots, M_{(m,0)} = C_{(m,0)} \oplus M_m = \bigvee_{i=1}^m C_{(m,0)}^i \oplus M_m).$$

随机编码系数分量累积异或向量 $V_{(i,0)}$ 由编码系数 $C_{(i,0)}$ 的相关分量组成, 则随机编码系数分量矩阵 V_{Alice} 为

$$V_{\text{Alice}} = (V_{(1,0)} = (C_{(1,0)}^1, C_{(2,0)}^1, \dots, C_{(m,0)}^1), \\ V_{(2,0)} = (C_{(1,0)}^2, C_{(2,0)}^2, \dots, C_{(m,0)}^2), \dots, V_{(m,0)} = (C_{(1,0)}^m, C_{(2,0)}^m, \dots, C_{(m,0)}^m)).$$

如图 1 所示, 发送匿名组的出口节点将 $\langle M_{(1,0)}, V_{(1,0)} \rangle, \langle M_{(2,0)}, V_{(2,0)} \rangle, \dots, \langle M_{(m,0)}, V_{(m,0)} \rangle$ 分散到不同的匿名链路中传输, 即 Alice 生成编码消息向量 M_{Alice} 和随机编码系数分量矩阵 V_{Alice} , 并通过发送伪装算法生成匿名通信消息, 发送匿名链路中各节点根据消息转发策略对其进行匿名转发, 在编码匿名转发网络中编码分片消息 $M_{(i,0)}$ 和随机编码系数分量累积异或向量 $V_{(i,0)}$ 将沿第 i 条匿名链路传输.

3.3 编码匿名转发网络的转发策略

如图 1 所示, 转发网络中各匿名链路的第 1 个节点 $O_{(i,1)}$ 直接从信源节点 ($O_{(i,1)}$ 认为其所接收的消息是由信源节点直接为其发送) 接收消息 $\{M_{(i,0)}, V_{(i,0)}\}$, 而其他节点 $O_{(i,j)} (i=1, 2, \dots, m; j=2, 3, \dots, n)$ 则从其直接前驱节点 $O_{(i,j-1)}$ 接收消息 $\{M_{(i,j-1)}, V_{(i,j-1)}, C_{(i,j-1)}^i\}$, 同时分别从其他 $m-1$ 条链路中接收到其前驱节点 $O_{(k,j-1)} (k=1, 2, \dots, m, k \neq i)$ 的编码系数分量 $C_{(k,j-1)}^i$.

编码匿名转发网络中各节点的转发策略主要包含以下步骤:

步骤 1 节点 $O_{(i,j)}$ 选取长度为 L 的随机编码系数 $C_{(i,j)}$ 对接收的编码分片消息 $M_{(i,j-1)}$ 按式 (2) 进行异或编码;

$$M_{(i,j)} = C_{(i,j)} \oplus M_{(i,j-1)} (i = 1, 2, 3, \dots, m; j = 1, 2, \dots, n). \quad (2)$$

步骤 2 计算编码系数分量的累积异或向量 $V_{(i,j)}$.

$V_{(i,j)}$ 的计算根据匿名链路的首节点 $O_{(i,1)}$ 和中间节点 $O_{(i,j)} (j=2, 3, \dots, n)$ 的不同计算策略分两种情况讨论:

① 节点 $O_{(i,1)}$ 的唯一前驱节点是信源节点, 即编码匿名转发网络中各链路的第 1 个节点 $O_{(i,1)}$ 从信源节点接收 $\{M_{(i,0)}, V_{(i,0)}\}$, 因此 $V_{(i,1)} = V_{(i,0)}$.

伪装算法的伪代码表示如下所述:

Begin

1: Initialization parameters(m, n, L_S, L_R, M);

2: $M = \text{Message} \oplus H(\text{ID}_{\text{Bob}})$ // ID_{Bob} 为信宿节点的身份信息, 即对 Alice 的原始通信消息 Message 进行异或编码产生匿名通信消息 M .

3: $M_1, M_2, \dots, M_m = f(M, m)$, and the length of $M_i (i = 1, 2, \dots, m)$ is L ;

4: **For** $i=1$ to $i = m$

$C_{(i,0)}$ is a random number, which is the coefficient for network coding;

Divided the $C_{(i,0)}$ into m component($C_{(i,0)}^1, C_{(i,0)}^2, \dots, C_{(i,0)}^m$), The length of last one is $L - (m - 1) \lfloor \frac{L}{m} \rfloor$, and the other length is $\lfloor \frac{L}{m} \rfloor$;

End For //产生随机编码系数 $C_{(i,0)}$, 并将其按二进制位等分成 m 个编码系数分量 $C_{(i,0)}^1, C_{(i,0)}^2, \dots, C_{(i,0)}^m$.

5: **For** $i=1$ to $i = m$

$M_{(i,0)} = C_{(i,0)} \oplus M_i$;

$V_{(i,0)} = (C_{(1,0)}^i, C_{(2,0)}^i, C_{(3,0)}^i, \dots, C_{(m,0)}^i)$;

End For//生成编码分片消息 $M_{(i,0)}$ 和累积异或向量 $V_{(i,0)}$.

6: $M_{\text{Alice}} = (M_{(1,0)}, M_{(2,0)}, \dots, M_{(m,0)})$, $V_{\text{Alcie}} = (V_{(1,0)}, V_{(2,0)}, \dots, V_{(m,0)})$ and $\text{IP}_{\text{Alcie}} = (V_{O(1,1)}, V_{O(2,1)}, \dots, V_{O(m,1)})$;

7: $\text{Data} = M_{\text{Alice}} || V_{\text{Alcie}} || \text{IP}_{\text{Alcie}}$;

8: $\text{Data} = E\{K_{(\text{Alice}, \text{Node}(\text{Ls}))}, \text{Data}\}$;

9: **For** $i = L_S - 1$ to $i=1$ //Alcie 封装匿名通信数据. 信源节点 Alice 使用这些节点建立发送匿名通信链路, 因此 L_S 也是发送匿名通信链路的长度, 为使表述统一称 L_S 为发送匿名组节点数.

$\text{Data} = E\{K_{(\text{Alice}, \text{Node}(i))}, \text{the IP address of Node}_{(i+1)} || \text{Data}\}$;

End For // $K_{(\text{Alice}, \text{Node}(i))}$ 为 Alice 与节点 $\text{Node}_{(i)}$ 基于改进 ECDH 算法协商的会话密钥.

End

发送匿名组中消息转发策略的伪代码表示如下所述:

Begin

1: $\text{Node}_{(1)}$ get Data from Alice;

2: $\text{Data}' = D\{K_{(\text{Alice}, \text{Node}(1))}, \text{Data}\}$;

3: $\text{Node}_{(1)}$ get the IP address of $\text{Node}_{(2)}$ from Data' , and submit the response data to $\text{Node}_{(2)}$;

4: **For** $J=2$ to $J = L_S - 1$

$\text{Node}_{(J)}$ get data from $\text{Node}_{(J-1)}$;

$\text{Data}' = D\{K_{(\text{Alice}, \text{Node}(J))}, \text{Data}'\}$;

$\text{Node}_{(J)}$ get the IP address of $\text{Node}_{(J+1)}$ from Data' , and submit the response data to $\text{Node}_{(J+1)}$;

End For

5: $\text{Node}_{(L_S)}$ get data from $\text{Node}_{(L_S-1)}$;

6: Data' = $D\{K_{(Alice, Node(Ls))}, \text{Data}'\}$;

7: Node_(Ls) get the $O_{(i,1)}$'s IP address from Data', and submit the response data to $O_{(i,1)}$ ($i = 1, 2, \dots, m$);

End

其中, $O_{(i,1)}$'s IP address 即为发送匿名链路出口节点的路由表.

节点 $O_{(i,1)}$ 将随机编码系数 $C_{(i,1)}$ 等分成 m 个编码系数分量 $C_{(i,1)}^1, C_{(i,1)}^2, \dots, C_{(i,1)}^m$. $O_{(i,1)}$ 发送消息 $\{M_{(i,1)}, V_{(i,1)}, C_{(i,1)}^i\}$ 到其直接后继节点 $O_{(i,2)}$, 同时沿第 k 条链路发送随机编码系数分量 $C_{(i,1)}^k$ ($k=1, 2, 3, \dots, m$, 且 $k \neq i$) 到其他后继节点 $O_{(k,2)}$.

② 节点 $O_{(i,J)}$ 收到其直接前驱节点的编码分片消息 $M_{(i,J-1)}$, 编码系数分量累积异或向量 $V_{(i,J-1)}$ 和随机编码系数分量 $C_{(i,J-1)}^i$, 同时接收到其他前驱节点 $O_{(k,J-1)}$ 的随机编码系数分量 $C_{(k,J-1)}^i$ ($k=1, 2, 3, \dots, m$, 且 $k \neq i$). 节点 $O_{(i,J)}$ 将 $C_{(i,J)}$ 等分成 m 个编码系数分量 $C_{(i,J)}^1, C_{(i,J)}^2, \dots, C_{(i,J)}^m$.

节点 $O_{(i,J)}$ 将接收到的编码系数分量组成向量 $Z_{O_{(i,J)}} = (C_{(1,J-1)}^i, C_{(2,J-1)}^i, \dots, C_{(m,J-1)}^i)$. 节点 $O_{(i,J)}$ 按式 (3) 计算随机编码系数分量累积异或向量 $V_{(i,J)}$,

$$V_{(i,J)} = Z_{O_{(i,J)}} \oplus V_{(i,J-1)} (i = 1, 2, \dots, m, J = 2, \dots, n), \quad (3)$$

即有:

$$\begin{aligned} V_{(1,J)} &= \left(C_{(1,J-1)}^1 \oplus \bigoplus_{t=0}^{J-2} C_{(1,t)}^1, C_{(2,J-1)}^1 \oplus \bigoplus_{t=0}^{J-2} C_{(2,t)}^1, \dots, C_{(m,J-1)}^1 \oplus \bigoplus_{t=0}^{J-2} C_{(m,t)}^1 \right) \\ &= \left(\bigoplus_{t=0}^{J-1} C_{(1,t)}^1, \bigoplus_{t=0}^{J-1} C_{(2,t)}^1, \dots, \bigoplus_{t=0}^{J-1} C_{(m,t)}^1 \right); \dots; \\ V_{(m,J)} &= \left(C_{(1,J-1)}^m \oplus \bigoplus_{t=0}^{J-2} C_{(1,t)}^m, C_{(2,J-1)}^m \oplus \bigoplus_{t=0}^{J-2} C_{(2,t)}^m, \dots, C_{(m,J-1)}^m \oplus \bigoplus_{t=0}^{J-2} C_{(m,t)}^m \right) \\ &= \left(\bigoplus_{t=0}^{J-1} C_{(1,t)}^m, \bigoplus_{t=0}^{J-1} C_{(2,t)}^m, \dots, \bigoplus_{t=0}^{J-1} C_{(m,t)}^m \right). \end{aligned}$$

步骤 3 节点 $O_{(i,j)}$ 计算生成编码分片消息 $M_{(i,j)}$ 和随机编码系数分量累积异或向量 $V_{(i,j)}$ 后查询路由表即可获知所有后继节点的网络地址 (其中节点 $O_{(i,I)}$ ($I=1, 2, \dots, n-1$) 以分链路转发方式通信; 节点 $O_{(i,n)}$ 以广播方式通信), 将 $M_{(i,j)}$, $V_{(i,j)}$ 和编码系数分量 $C_{(i,j)}^i$ 通过第 i 条链路传递给下一跳节点 $O_{(i,j+1)}$, 其他的编码系数分量 $C_{(i,j)}^k$ ($k=1, 2, \dots, m; k \neq i$) 将沿第 k 条链路传递给节点 $O_{(k,j+1)}$. 各匿名链路中第 n 个节点 $O_{(i,n)}$ 的后继节点即为接收匿名组中的成员, 因此 $O_{(i,n)}$ 将消息 $B_i = \{M_{(i,n)}, V_{(i,n)}, C_{(i,n)}\}$ 以广播的方式发送给接收匿名组.

3.4 信宿节点的解码策略

由于编码匿名转发网络出现网络差错的概率是可忽略的, 所以信宿节点 Bob 能够接收到所有的编码分片消息 $M_{(i,n)}$ 、随机编码系数分量累积异或向量 $V_{(i,n)}$ 和编码系数 $C_{(i,n)}$ ($i=1, 2, \dots, m$).

定理 1 在编码匿名转发网络不存在差错、延迟等情况时, 信宿节点能够正确解码编码分片消息并还原信源节点的原始通信消息 Message.

证明 在编码匿名转发网络不存在差错、延迟等情况时, 信宿节点 Bob 能够完全接收 m 条匿名链路所发送的编码分片消息 $M_{(i,n)}$ 、编码系数分量的累积异或向量 $V_{(i,n)}$ 和节点 $O_{(i,n)}$ 的随机编码系

数 $C_{(i,n)} (i=1, 2, \dots, m)$, 则 $M_{(i,n)} = \bigoplus_{j=0}^n C_{(i,j)} \oplus M_i$, 其中 $C_{(i,j)} = \bigoplus_{k=1}^m C_{(i,j)}^k$, $(i=1, 2, \dots, m, j=0, 1, 2, \dots, n)$.

Bob 进行编码分片消息解码前的准备操作:

(1) Bob 接收的编码分片消息向量 M_{Bob} 为

$$M_{\text{Bob}} = (M_{(1,n)}, M_{(2,n)}, \dots, M_{(m,n)}) = \left(\bigoplus_{j=0}^n C_{(1,j)} \oplus M_1, \bigoplus_{j=0}^n C_{(2,j)} \oplus M_2, \dots, \bigoplus_{j=0}^n C_{(m,j)} \oplus M_m \right).$$

(2) Bob 接收的节点 $O_{(i,n)}$ 的随机编码系数向量 Z_{Bob} 为

$$Z_{\text{Bob}} = (C_{(1,n)}, C_{(2,n)}, C_{(3,n)}, C_{(4,n)}, \dots, C_{(m,n)}).$$

(3) Bob 接收的随机编码系数分量的累积异或向量 $V_{(i,n)}$ 分别为

$$V_{(1,n)} = \left(\bigoplus_{t=0}^{n-1} C_{(1,t)}^1, \bigoplus_{t=0}^{n-1} C_{(2,t)}^1, \dots, \bigoplus_{t=0}^{n-1} C_{(m,t)}^1 \right), \dots, V_{(m,n)} = \left(\bigoplus_{t=0}^{n-1} C_{(1,t)}^m, \bigoplus_{t=0}^{n-1} C_{(2,t)}^m, \dots, \bigoplus_{t=0}^{n-1} C_{(m,t)}^m \right).$$

当 $j=0$ 时, $C_{(i,j)}^N$ 是 Alice 的随机编码系数分量, 且由第 N 条链路传输该分量; 当 $j \neq 0$ 时, $C_{(i,j)}^N$ 为节点 $O_{(i,j)}$ 的随机编码系数分量, 且由第 N 条链路进行传输.

信宿节点 Bob 通过下述步骤解码编码分片消息还原 Alice 的原始通信消息 M :

步骤 1 Bob 对编码系数分量的累积异或向量 $V_{(i,n)} (i=1, 2, \dots, m)$ 进行拼接运算, 即消息还原向量 V_{Bob} 为

$$\begin{aligned} V_{\text{Bob}} &= V_{(1,n)} \| V_{(2,n)} \| V_{(3,n)} \| \dots \| V_{(m,n)} \\ &= \left(\bigoplus_{t=0}^{n-1} C_{(1,t)}^1 \| \bigoplus_{t=0}^{n-1} C_{(1,t)}^2 \| \dots \| \bigoplus_{t=0}^{n-1} C_{(1,t)}^m, \bigoplus_{t=0}^{n-1} C_{(2,t)}^1 \| \bigoplus_{t=0}^{n-1} C_{(2,t)}^2 \| \dots \| \bigoplus_{t=0}^{n-1} C_{(2,t)}^m, \dots, \right. \\ &\quad \left. \bigoplus_{t=0}^{n-1} C_{(m,t)}^1 \| \bigoplus_{t=0}^{n-1} C_{(m,t)}^2 \| \dots \| \bigoplus_{t=0}^{n-1} C_{(m,t)}^m \right) \\ &= \left(\bigoplus_{t=0}^{n-1} C_{(1,t)}, \bigoplus_{t=0}^{n-1} C_{(2,t)}, \bigoplus_{t=0}^{n-1} C_{(3,t)}, \dots, \bigoplus_{t=0}^{n-1} C_{(m,t)} \right). \end{aligned}$$

步骤 2 Bob 将消息还原向量 V_{Bob} 与节点 $O_{(i,n)}$ 的随机编码系数向量 Z_{Bob} 进行异或运算, 则有

$$\begin{aligned} V_{\text{Bob}} \oplus Z_{\text{Bob}} &= \left(\bigoplus_{t=0}^{n-1} C_{(1,t)} \oplus C_{(1,n)}, \bigoplus_{t=0}^{n-1} C_{(2,t)} \oplus C_{(2,n)}, \dots, \bigoplus_{t=0}^{n-1} C_{(m,t)} \oplus C_{(m,n)} \right) \\ &= \left(\bigoplus_{t=0}^n C_{(1,t)}, \bigoplus_{t=0}^n C_{(2,t)}, \dots, \bigoplus_{t=0}^n C_{(m,t)} \right). \end{aligned}$$

步骤 3 Bob 将编码消息向量 M_{Bob} 与向量 $V_{\text{Bob}} \oplus Z_{\text{Bob}}$ 进行异或运算, 则有

$$\begin{aligned} M_{\text{Bob}} \oplus (V_{\text{Bob}} \oplus Z_{\text{Bob}}) &= \left(M_{(1,n)} \oplus \bigoplus_{t=0}^n C_{(1,t)}, M_{(2,n)} \oplus \bigoplus_{t=0}^n C_{(2,t)}, \dots, M_{(m,n)} \oplus \bigoplus_{t=0}^n C_{(m,t)} \right) \\ &= \left(\bigoplus_{t=0}^n C_{(1,t)} \oplus \bigoplus_{j=0}^n C_{(1,j)} \oplus M_1, \bigoplus_{t=0}^n C_{(2,t)} \oplus \bigoplus_{j=0}^n C_{(2,j)} \oplus M_2, \dots, \right. \\ &\quad \left. \bigoplus_{t=0}^n C_{(m,t)} \oplus \bigoplus_{j=0}^n C_{(m,j)} \oplus M_m \right) \\ &= (M_1, M_2, \dots, M_m). \end{aligned}$$

即 Bob 获得 Alice 发送匿名通信消息的 m 份分片消息 $M_1, M_2, \dots, M_m$.

步骤 4 Bob 根据分片消息 $M_1, M_2, \dots, M_m$ 通过信息分割函数的逆函数 $f^{-1}()$ 还原原始通信消息 M , 则有

$$M = f^{-1}(M_1, M_2, \dots, M_m).$$

步骤 5 Bob 根据自己的身份信息 ID_{Bob} 还原 Alice 的原始通信消息 Message,

$$\text{Message} = M \oplus H(ID_{\text{Bob}}).$$

4 模型分析

本节对 ACM-NC 的匿名性、安全性及计算效率等进行理论分析和模拟仿真实验.

4.1 匿名性分析

(1) 发送者匿名和接收者匿名

由于信源节点随机选取一定数量的可信节点构建发送匿名组, 因而其建立的发送匿名链路具有不可追踪性; 同时, 由于匿名通信消息是由信源节点层层嵌套加密生成, 而链路的中间节点仅能知晓自己的直接前驱和直接后继, 不可能知道链路中的其他节点, 即使外部观察者侦听到匿名通信消息, 其所看到数据报中的 IP 地址并不是信源节点和信宿节点的真实地址, 因此发送匿名组可满足信源节点和信宿节点的匿名性需求.

信源节点在建立编码匿名转发网络的同时, 协助各节点建立通信路由表. 在匿名通信过程中节点 $O_{(i,j)}$ 仅知晓前驱节点 $O_{(i,j-1)}$ 和后继节点 $O_{(i,j+1)}$ 的相关地址信息, 无法获知编码转发网络中其他节点的相关信息, 外部观察者即使侦听到通信数据, 其所看到 IP 数据报中的地址并非信源节点和信宿节点的地址, 即使攻击者控制转发网络中第 i 条链路的第 1 个节点 $O_{(i,1)}$, 其仅能获得发送匿名组出口节点的地址信息; 即使攻击者控制转发网络中第 i 条链路的出口节点 $O_{(i,n)}$, 其仅能获知接收匿名组的广播地址, 因此编码匿名转发网络可满足信源节点和信宿节点的匿名性需求.

在接收匿名组中, 除接收者之外的其他员认为获得的信源地址实际上是编码匿名转发网络出口节点的地址信息; 并且当接收匿名组成员达到一定数量时, 攻击者猜中信宿节点的概率是可忽略的, 因此, 接收匿名组也可满足信源节点和信宿节点的匿名性需求.

(2) 通信消息的匿名性

信源节点将原始通信消息分割成分片消息后, 根据发送匿名组中各节点的先后顺序使用相应的会话密钥进行层层嵌套加密, 在发送匿名组中每经过一个节点解密一次, 直至出口节点时才将所有的嵌套加密处理完. 同时, 其加密传输方式可有效阻止窃听和流量分析等攻击行为, 即发送匿名组可满足通信消息的匿名性需求.

发送匿名组的出口节点将分片消息和相关参数分量通过匿名转发网络中不同的链路发往信宿节点, 在编码转发网络中各转发节点由于无法掌握所有的分片消息和节点的随机编码系数而无法解码还原信源节点的原始通信消息, 因此编码匿名转发网络能满足通信消息的匿名性需求.

接收匿名组中各成员虽完全接收所有的分片消息和相关参数, 但由于除信宿节点之外的各成员均很难准确定位信宿节点而无法获知其身份信息, 导致无法完全解密信源节点的匿名通信信息, 即接收匿名组可满足通信消息的匿名性需求.

(3) 匿名度仿真

图 2 P 和 L_S 对匿名度的影响Figure 2 Effects of P and L_S on the anonymity degree D 图 3 m 和 n 对匿名度的影响Figure 3 Effects of m and n on the anonymity degree D

在编码匿名转发网络中节点 $O_{(i,j)}$ 仅知道自己的前驱节点 $O_{(k,j-1)}$ 和后继节点 $O_{(k,j+1)}$, 无法获悉转发网络中的其他节点的相关信息, 因而攻击者即使侦听到通信数据, 其所看到 IP 数据报中的地址也并非信源节点和信宿节点的地址, 即使其控制了转发网络中第 i 条路径的第 1 个节点 $O_{(i,1)}$ 和最后一个节点 $O_{(i,n)}$, 也无法获知信源节点和信宿节点的真实 IP 地址, 即编码匿名转发网络满足绝对匿名的要求。

本节将在发送匿名组、接收匿名组和编码匿名转发网络存在攻击者的情况下, 对本文 ACM-NC 的匿名性进行仿真分析。

定义 8 发送匿名组和接收匿名组的匿名度 D_S 和 D_R 分别为信源节点和信宿节点的位置、身份等隐私信息被攻击者获悉的概率。当 D_S 和 D_R 趋近于 0 时, 发送匿名组和接收匿名组的匿名性将达到绝对匿名的等级。

若发送匿名组和接收匿名组存在攻击者时, 根据针对合谋攻击进行匿名度分析的方法^[25]可知发送匿名组的匿名度为: $D_S = \frac{(1-P)^2}{(1-PL_S P)(1-PL_S P+1)}$, 其中 L_S 是发送匿名组节点数, P 为节点是有效节点的概率, 即发送匿名组的匿名链路中恶意节点数为 $L_S(1-P)$ 。如图 2 仿真表明, 发送匿名组的匿名度随 L_S 和 P 的增大而减小, 匿名性能越佳, 并且受 P 的影响较大。当 $L_S \geq 10$, $P \geq 0.75$ 时匿名度大小趋近于 0, 即发送匿名组的匿名度已接近绝对匿名的等级。则当 $P \geq 0.75$ 时, 信源节点选择 10 个节点即可建立高匿名性的发送匿名组。

由广播通信的特点可知, 接收匿名组的匿名度为 $D_R = \frac{1}{L_R}$, 其中 L_R 是接收匿名组成员数。

定义 9 编码匿名转发网络的匿名度 D_{Net} , 即为信源节点原始通信消息经编码匿名转发网络传输时被攻击者合谋解码的概率。当 D_{Net} 趋近于 0 时, 转发网络的匿名性将接近绝对匿名。

在编码匿名转发网络中, 攻击者若要获知信源节点与信宿节点间的通信消息, 则攻击者必须完全掌控转发网络中的 m 个节点 $O_{(i,k)}$ ($i=1, 2, \dots, m$), 并且各受控节点必须处于每条匿名链路的不同转发位置。同时, 攻击者应完全获知途经这些节点的编码分片消息 $M_{(i,k)}$ 、随机编码系数分量累积异或向量 $V_{(i,k)}$ 和前驱节点 $O_{(i,k-1)}$ 的随机编码系数分量, 以及信宿节点的身份信息, 才能通过相关计算 (与信宿节点的计算方法相同) 还原通信消息 M 。

攻击者控制转发网络第 k 列节点的概率为 $\frac{n}{C_{mn}^m}$, 那么转发网络的匿名度为 $D_{NET} = \frac{m!n(mn-m)!}{(mn)!}$,

图 4 L_S 和 P 对匿名度的影响

Figure 4 Effects of L_S and P on the anonymity degree of ACM-NC ($m=4$, $n=3$)

图 5 m 和 n 对匿名度的影响

Figure 5 Effects of m and n on the anonymity degree ($L_S = 10$, $P = 0.75$)

其中 m 为编码匿名转发网络中链路数, n 为编码匿名转发网络的链路长度. 如图 3 仿真表明, 编码匿名转发网络的匿名度随 m 和 n 的增大而减小, 受 m 的影响较大. 但当 $m \geq 4$, $n \geq 3$ 时匿名度大小趋近于 0, 趋于绝对匿名, 且此时匿名度已不受 m 和 n 的影响, 即信源节点选择 12 ($m=4$, $n=3$) 个节点即可建立绝对匿名的转发网络.

编码匿名转发网路具有较强的匿名性, 选取少量节点就可满足绝对匿名通信的需求, 因此在现实网络环境中易部署, 具有较强的推广性.

定义 10 ACM-NC 的匿名度 D , 即为信源节点、信宿节点和匿名通信消息都不被攻击者识别的概率. 当 D 趋近于 1 时, ACM-NC 的匿名性将达到绝对匿名的等级.

当发送匿名组和接收匿名组中存在恶意攻击者, 并且攻击者对转发网络可进行合谋攻击时, 则本文 ACM-NC 的匿名度 D 为: $D = \left[1 - \frac{(1-P)^2}{(1-PL_S P)((1-PL_S P+1))} \right] \left[1 - \frac{1}{L_R} \right] \left[1 - \frac{m!n(mn-m)!}{(mn)!} \right]$. 图 4 给出了当转发网络链路数 $m(m=4)$ 和链路长度 $n(n=3)$ 固定时, 随着 L_S 和 P 的增加, 匿名度 D 逐渐增加, ACM-NC 的匿名性增强, 且 P 的变化对匿名度的大小影响较大. 图 5 给出了当 L_S ($L_S = 10$) 和 P ($P = 0.75$) 固定时, 随着 m 和 n 的增加, 匿名度 D 大小基本不发生变化, 即此时可忽略 m 和 n 的变化对 ACM-NC 的匿名性影响. 由图 4 和图 5 可知, 随着 L_R 的增加, 匿名度 D 逐渐增加, 并且 L_R 对匿名度的影响较大; 当 L_S , P 和 L_R 达到一定值时 ($L_S \geq 10$, $P \geq 0.75$, $L_R \geq 10$), 编码匿名转发网络的链路数 m 和链路长度 n 的取值对匿名度的影响是可忽略.

由于 L_S 过长会使通信时延变大, 因而 L_S 不宜过大, 选择适当长度即可, 以免造成通信时延的增加. 因此, 信源节点选择与其相同区域的节点 (即邻居节点) 建立发送匿名组, 以降低发送匿名组对通信时延的影响; 接收匿名组成员数 L_R 对匿名度影响较大, 由于节点 $O_{(i,n)}$ 以广播通信方式将通信消息发送给接收匿名组中的每个成员, 因此 L_R 的取值并未影响通信时延, 所以可适当选取较大的 L_R 以保证 ACM-NC 达到更好的匿名效果.

虽说信源节点可选择同一区域的邻居可信节点建立发送匿名组, 理论上存在降低时延的可能性, 但 L_S 过长会导致通信时延的增加, 如图 4 所示, $L_S \geq 10$ 时即可满足 ACM-NC 对发送匿名组的匿名性需求, 因此在应用中根据用户的实际需求选择 L_S 的最佳值, 主要有 3 种情况: (1) 若用户追求高匿名性而对通信效率的需求较弱, 则可选择较多的节点完成发送匿名组的构建, 即 $L_S > 10$; (2) 若用户

希望获得匿名性的同时, 兼顾通信效率, 则选择即兼顾通信效率又能够满足基本匿名性需求的节点数构建发送匿名组, 即 $L_S=10$; (3) 若用户对匿名性要求较弱, 更加关注通信效率, 此时发送伪装组的节点数越少越好, 即 $L_S < 10$. 因此在本文 ACM-NC 中最佳的 L_S 值需根据用户对匿名性和通信效率的实际需求而确定.

综上所述: 当 $L_S \geq 10$, $P \geq 0.75$, $L_R \geq 10$, $m=4$ 和 $n=3$ 时, 本文 ACM-NC 具有较强的匿名性, 且其匿名性趋于绝对匿名, 即 ACM-NC 无需可信密钥分发中心协助即可建立高匿名性通信链路, 并且具有部署代价小, 易推广应用的优点.

4.2 安全性分析

(1) 发送匿名组安全性

(a) 消息的加密传输. 信源节点将分片消息和随机编码系数等通信消息嵌套加密封装后, 通过发送匿名组进行转发. 嵌套加密封装是将通信数据、发送匿名组出口地址和信源地址等包头信息, 按发送匿名组中各节点的先后顺序, 使用相应的会话密钥将其层层嵌套加密形成匿名通信消息的过程, 匿名消息每经过一个可信节点被解密一层, 直至出口节点时才将嵌套加密处理完. 加密传输能有效阻止恶意节点的窃听和流量分析等攻击行为, 即使某个节点被攻击者所控制, 由于该节点仅掌握自己的会话密钥, 攻击者只能从数据包中得知该节点直接前驱和直接后继的相关信息, 无法获知通信消息、信源节点和信宿节点的隐私信息, 因此除非攻击者控制该链路中所有的节点, 才能获知具体的通信信息, 而这在现实中是很难实现的.

(b) 抗被动攻击. 若窃听者捕获到发送匿名链路中某节点的会话密钥协商参数, 由于没有信源节点的相应参数, 无法计算相应的会话密钥, 而无法正确解密匿名通信消息, 因此仅有合法的匿名链路节点才能得到正确的匿名通信消息; 同时发送匿名链路可抵抗流量分析等攻击.

(c) 抗主动攻击. 若窃听者捕获信源节点与节点 $\text{Node}_{(i)}$ 的会话密钥, 则其仅能获得 $\text{Node}_{(i+1)}$ 的地址信息, 并不能获得其他节点的任何信息. 若窃听者欲跳过节点 $\text{Node}_{(i+1)}$ 把下一节点设为 $\text{Node}_{(K)}$, 由于 $\text{Node}_{(K)}$ 无法获悉正确的会话密钥, 无法对匿名通信消息进行处理和转发, 则 $\text{Node}_{(K)}$ 拒绝转发数据, 保证了数据转发链路的真实性.

(d) 路由的可鉴别性. 发送匿名链路中的各节点均能确认其是匿名通信链路的中间节点, 并且每个节点都可确认匿名通信消息来源的真实性. 由抗主动攻击分析可知, 当攻击者将非链路中节点作为下一跳节点时, 由于其无法获知正确的会话密钥, 将无法正确转发匿名通信消息.

(2) 编码匿名转发网络的安全性

(a) 节点的接入度量. 转发网络建立时, 信源节点对接入节点基于可信性验证策略进行平台可信性验证, 仅将可信节点接入转发网络. 节点的接入度量机制防止了非法节点的接入, 确保了转发网络的安全性和可靠性. 文献 [26] 详细叙述了可信性验证策略及相关关键技术, 篇幅所限, 本文不再赘述.

(b) 信息的极少量泄露. 发送匿名链路和转发网络中各节点仅知晓其前驱节点和后继节点的相关信息, 无法获知其他节点及信源节点与信宿节点的任何隐私信息.

(c) 抗合谋攻击.

定理 2 信源节点通过编码匿名转发网络发送通信消息 Message 的过程中, 如果编码匿名转发网络有 m 条匿名链路, 且每条链路中有 n 个节点, 当转发网络中各节点进行合谋攻击时, 信源节点的通信消息 Message 编码可解的充要条件是每条匿名链路中至少存在一个合谋成员节点 $O_{(i,p)} (i=1, 2, \dots, m, p \in [1, n])$, 并且各合谋成员必须处于每条匿名链路的相同转发位置, 同时攻击者还需获悉信宿节点的身份信息.

证明 A 必要性

节点 $O_{(i,p)}$ 收到直接前驱节点 $O_{(i,p-1)}$ 发送的编码分片消息 $M_{(i,p-1)}$ 和编码系数分量的累积异或向量 $V_{(i,p-1)}$ 及编码系数分量 $C_{(i,p-1)}^i$, 同时 $O_{(i,p)}$ 还收到其他前驱节点 $C_{(h,p-1)}$ 的随机编码系数分量 $C_{(h,p-1)}^i$, 其中 $h \neq i$.

① 当且仅当各合谋成员处于每条匿名链路相同的转发位置时, 各合谋成员才能通过已有的累积异或向量还原各链路中相关节点的随机编码系数, 否则将无法还原随机编码系数, 更无法进行编码分片消息的解码.

若合谋成员中至少存在一个节点 $O_{(L,Q)}$ 与 $O_{(i,p)}$ 在匿名链路中所处的位置不相同, 则 $p \neq Q$ 且 $i \neq L$, 节点 $O_{(i,p)}$ 进行合谋攻击时, 无法通过拼接累积异或向量 $V_{(1,p)}, \dots, V_{(L-1,p)}, V_{(L,Q)}, V_{(L+1,p)}, \dots, V_{(m,p)}$ 还原各链路中相关节点的随机编码系数累积异或向量 $(\bigoplus_{t=0}^{p-1} C_{(1,t)}, \bigoplus_{t=0}^{p-1} C_{(2,t)}, \dots, \bigoplus_{t=0}^{p-1} C_{(m,t)})$, 即等式 $(\bigoplus_{t=0}^{p-1} C_{(1,t)}, \bigoplus_{t=0}^{p-1} C_{(2,t)}, \dots, \bigoplus_{t=0}^{p-1} C_{(m,t)}) = (\big\|_{t=0}^{L-1} V_{(t,p)} \big\| V_{(L,Q)} \big\| \big\|_{t=L+1}^m V_{(t,p)})$ 不成立. 因此, 当攻击者对编码转发网络进行合谋攻击时, 各链路的合谋成员必须处于匿名链路的相同位置.

② 若编码匿名转发网络中第 $k(k \neq i)$ 条匿名链路为安全可靠的匿名通信链路, 即该链路中无合谋成员, 则节点 $O_{(i,p)}$ 无法掌握该链路的随机编码系数 $C_{(k,x)}(x=1, 2, \dots, p-1)$, 则节点 $O_{(i,p)}$ 无法解码编码分片消息 $M_{(k,p-1)}$, 也无法获知分片消息 M_k , 则无法还原原始匿名通信消息 M ; 若第 k 条链路中节点 $O_{(k,p)}$ 不对其他链路合谋成员共享数据, 节点 $O_{(i,p)}$ 同样无法还原 M ; 因此当转发网络中第 $k(k \neq i)$ 条是安全可靠的匿名链路, 或者节点 $O_{(k,p)}$ 不对外共享数据信息, 节点 $O_{(i,p)}$ 将无法获知分片消息 M_k 的相关信息, 等式 $M = f^{-1}(M_1, M_2, \dots, M_{k-1}, M_{k+1}, \dots, M_m)$ 不成立, 则节点 $O_{(i,p)}$ 无法还原原始匿名通信消息 M .

当攻击者对转发网络进行合谋攻击时, 每条匿名链路必须至少存在一个合谋攻击成员, 并且由 ① 可知它们在匿名链路中所处的位置必须相同.

③ 若原始匿名通信消息 M 在节点 $O_{(i,p)}$ 处被还原, 显然节点 $O_{(i,p)}$ 需掌握分片消息 $M_1, M_2, \dots, M_m$. 由 ① 和 ② 可知只有在编码匿名转发网络中每条匿名链路的相同位置存在一个合谋攻击成员时, 节点 $O_{(i,p)}$ 才能通过拼接随机编码系数分量的累积异或向量 $V_{(1,p)}, V_{(2,p)}, \dots, V_{(m,p)}$ 生成随机编码系数的累积异或向量 $(\bigoplus_{t=0}^{p-1} C_{(1,t)}, \bigoplus_{t=0}^{p-1} C_{(2,t)}, \dots, \bigoplus_{t=0}^{p-1} C_{(m,t)})$, 并用其解码编码消息 $M_{(1,p-1)}, M_{(2,p-1)}, \dots, M_{(m,p-1)}$ 获得分片消息 $M_1, M_2, \dots, M_m$. 节点 $O_{(i,p)}$ 基于分片信息还原原始匿名通信消息 M , 即等式 $M = f^{-1}(M_1, M_2, \dots, M_m)$ 成立.

④ 原始匿名通信消息 M 还原后, $O_{(i,p)}$ 只有在信宿节点身份信息的作用下才能还原出信源节点的真实通信消息 Message, 即节点 $O_{(i,p)}$ 通过 $\text{Message} = M \oplus H(\text{ID}_{\text{Bob}})$ 获得原始通信消息.

若想通过解码编码分片消息还原通信消息 Message, 其编码匿名转发网络中各匿名链路中至少存在一个合谋成员节点, 并且各合谋成员必须处于链路的相同转发位置, 同时攻击者还需获悉信宿节点的身份信息.

B 充分性

由于编码转发网络中各匿名链路中存在至少一个合谋成员, 并且各合谋成员处于每条匿名链路的相同转发位置, 因此第 i 条匿名链路中的合谋节点 $O_{(i,p)}$ 即可通过与其他合谋成员间的通信及数据共享而掌握编码匿名转发网络中各链路的累积异或向量 $(V_{(1,p)}, V_{(2,p)}, \dots, V_{(m,p)})$, 对其进行拼接运算生成随机编码系数的累积异或向量 $(\bigoplus_{t=0}^{p-1} C_{(1,t)}, \bigoplus_{t=0}^{p-1} C_{(2,t)}, \dots, \bigoplus_{t=0}^{p-1} C_{(m,t)})$, 基于随机编码系数累积异或向量解码编码消息 $M_{(i,p-1)}$ 获得分片消息 $M_i(i=1, 2, \dots, m)$, 则合谋成员在信宿节点身份信息的作用下

图 6 合谋成功的概率仿真

Figure 6 The simulation for success probability of conspiracy attack

即可还原信源节点的真实通信消息 Message.

节点 $O_{(i,p)}$ 通过下述计算即可还原信宿节点的原始通信消息 Message.

$$\left(\bigoplus_{t=0}^{p-1} C_{(1,t)}, \bigoplus_{t=0}^{p-1} C_{(2,t)}, \dots, \bigoplus_{t=0}^{p-1} C_{(m,t)} \right) = \bigoplus_{t=0}^{p-1} V_{(t,p)}; M_i = \bigoplus_{t=0}^{p-1} C_{(i,t)} \oplus M_{(i,p-1)} (i = 1, 2, \dots, m);$$

$$M = f^{-1}(M_1, M_2, M_3, M_4, \dots, M_m); \text{Message} = M \oplus H(\text{ID}_{\text{Bob}}).$$

当编码匿名转发网络中各匿名链路中存在至少一个合谋成员, 同时各合谋成员处于匿名链路的相同转发位置, 并且攻击者获知信宿节点的身份信息, 则此时合谋成员可获得信源节点的原始通信消息 Message.

综上所述: 当转发网络中各节点进行合谋攻击时, 信源节点的通信消息 Message 编码可解的充要条件是每条匿名链路中至少存在一个合谋成员, 并且各合谋成员必须处于每条匿名链路的相同转发位置, 同时攻击者还需获悉信宿节点的身份信息.

在编码匿名转发网络中, 各节点 $O_{(i,j)}$ 仅知道自己的前驱节点 $O_{(i,j-1)}$ 和后继节点 $O_{(i,j+1)}$, 不可能获悉转发网络中的其他节点, 外部观察者即使侦听到通信数据, 而他们所看到 IP 数据报中的地址信息并非 Alice 和 Bob 的地址, 也无法获知二者的相关身份信息. 当合谋成员对编码转发网络进行合谋攻击时, 其攻击成功的概率为 $\Gamma = \frac{n}{C_{mn}^m}$, 如图 6 仿真表明, 合谋攻击成功的概率随 m 和 n 的增大而减小, 且受 m 的影响较大; 当 $m=4, n=3$ 时攻击者合谋攻击成功的概率是可忽略, 并且随着 m 和 n 的增加, 攻击成功的概率不受 m 和 n 的影响. 因此信源节点选择 12 个节点即可建立绝对安全的编码匿名转发网络, 则编码匿名转发网络具有易构建和易推广的特点.

由于现实网络环境中攻击者很难在每条匿名链路的相同位置控制一个合谋节点, 因此攻击者很难通过控制节点对编码匿名转发网络进行合谋攻击; 并且仿真表明当 $m \geq 4$ 和 $n \geq 3$ 时, 进行合谋攻击时成功的概率是可忽略的. 因此编码匿名转发网络具有较强的抗合谋攻击能力.

4.3 保密性分析

本节从编码匿名转发网络中单节点解码和多节点联合解码两种情况分析 ACM-NC 的保密性.

(1) 单节点解码

定理 3 编码匿名转发网络中节点 $O_{(i,j)}$ 无法通过解码编码分片消息 $M_{(i,j)}$ 还原匿名通信消息 M , 即编码匿名转发网络中任意节点 $O_{(i,j)}$ 均无法还原信源节点的原始通信消息 Message.

证明 在编码匿名转发网络中, 各匿名链路的第 1 个节点 $O_{(i,1)}$ 接收 Alice 的编码分片消息 $M_{(i,0)}$ 和编码系数分量的累积异或向量 $V_{(i,0)}$, 节点 $O_{(i,1)}$ 由于无法通过拥有的 $V_{(i,0)}$ 还原编码系数 $C_{(i,0)}$, 所以不能直接解码编码分片消息 $M_{(i,0)}$, 则节点 $O_{(i,1)}$ 无法解码分片消息 M_i .

节点 $O_{(i,j)}$ 接收到直接前驱节点 $O_{(i,j-1)}$ 的编码分片消息 $M_{(i,j-1)}$ 和编码系数分量的累积异或向量 $V_{(i,j-1)}$ 及编码系数分量 $C_{(i,j-1)}^i$, 同时还收到节点 $O_{(k,j-1)}$ 的编码系数分量 $C_{(k,j-1)}^i$. 显然节点 $O_{(i,j)}$ 要解码 $M_{(i,j-1)}$ 需掌握随机编码系数 $C_{(i,x)} (x = 1, 2, \dots, j-1)$, 而节点 $O_{(i,j)}$ 仅掌握随机编码系数 $C_{(i,j)}$, 也无法通过已有的 $V_{(i,j-1)}$ 还原编码系数 $C_{(i,x)}$, 则节点 $O_{(i,j)}$ 无法还原分片消息 M_i .

若攻击者控制节点 $O_{(i,j)}$, 因节点 $O_{(i,j)}$ 所接收的编码分片消息是经过第 i 条链路中前 $j-1$ 个节点的编码处理. 仅当攻击者完全掌握第 i 条链路中前 $j-1$ 个节点的随机编码系数 $C_{(i,j)}$ 时, 才能还原分片消息 M_i , 然而节点 $O_{(i,j)}$ 仅知道自己的前驱结点 $O_{(i,j-1)}$ 和后继节点 $O_{(i,j+1)}$, 不可能获知转发网络中的其他节点, 这将对攻击者控制链路中其他节点的可行性提出考验, 因这在现实网络中很难实现, 同时攻击者也无法将已有信息与其他节点进行关联. 即使攻击者控制第 i 条链路中的所有节点, 也只能解码编码信息而获得分片消息 M_i , 而无法获知其他的分片消息, 则攻击者仍无法获知信源节点的原始匿名通信消息 M , 更无法获知原始通信消息 Message.

因此, 编码匿名转发网络中任意节点均无法通过解码编码分片消息还原信源节点的原始通信消息 Message.

(2) 多节点联合解码

定理 4 当 $m \geq 4, n \geq 3$ 时, 编码匿名转发网络中任意 $Y (Y \leq 0.7 mn)$ 个节点联合都无法通过解码编码消息还原匿名通信消息 M , 即无法还原信源节点的原始通信消息 Message.

证明 假设节点数 Y 占编码匿名转发网络节点总数的比例为 P . 下面将分类讨论在不同情况下 Y 个节点联合解码的可行性.

① $Y < m$. 信源节点通过信息分割策略将原始匿名通信消息 M 分割为 m 份分片消息 M_i , 并沿编码匿名转发网络的 m 条匿名链路发往信宿节点. 由定理 2 可知, 编码匿名转发网络中节点若想联合解码成功则每条链路上至少有一个参与者, 即当 $Y < m$ 时, Y 个节点无法解码还原信源节点的原始通信消息 Message.

② $Y = m$. 由定理 2 和匿名度仿真可知, 当信源节点建立的编码匿名转发网络满足 $m \geq 4$ 和 $n \geq 3$ 时, 转发网络中各节点进行联合解码的成功率是可忽略的, 因而节点无法通过联合解码而获得信源节点的通信消息, 即当 $Y = m$ 时, Y 个节点无法解码还原信源节点的原始通信消息 Message.

③ $Y > m$. 由定理 2 和匿名度仿真可知当 $Y > m$ 时, 多节点联合解码成功的概率为 $\beta = \frac{n C_{(m-1)n}^{Y-m}}{C_{mn}^Y}$, 本文对匿名链路数 m 、匿名链路长度 n 和联合解码节点数 Y 对 β 的影响关系进行了仿真.

如图 7 所示, 当 $m=4, n \geq 3$ 时, 编码匿名转发网络中 $Y (Y=0.7 mn)$ 个节点进行联合解码时其成功的概率低于 0.25; 如图 8 所示, 当 $m \geq 4, n=3$ 时, $Y (Y=0.7 mn)$ 个节点进行联合解码的成功率趋向于 0. ACM-NC 的保密性随 m 和 n 的增加而增强; 链路数 m 越大, 联合解码成功的条件越苛刻, 则联合解码成功的可能性就越低, 即 ACM-NC 的保密性受 m 的影响较大.

图 7 ACM-NC 保密性与 n 间关系 ($m=4$)

Figure 7 The relationship between ACM-NC confidentiality and n ($m=4$)

图 8 ACM-NC 保密性与 m 间关系 ($n=3$)

Figure 8 The relationship between ACM-NC confidentiality and m ($n=3$)

当 $m \geq 4, n \geq 3$, 编码匿名转发网络中 Y ($Y \leq 0.7mn$) 个节点进行联合解码时, ACM-NC 仍具有较强的保密性. 在现实网络中, 由于控制 70% 的节点进行联合解码具有一定的困难性, 因此编码匿名转发网络中节点无法通过联合解码而获得信源节点的原始通信消息 Message, 即当 $Y > m$ 时, Y 个节点联合解码还原信源节点的原始通信消息 Message 的概率是可忽略的.

由定理 3 和 4 可知, 信源节点选择 12 个可信节点即可构建具有强保密性的编码匿名转发网络. 当且仅当每条匿名链路的相同位置存在一个联合解码的节点时才能完全解码, 因此 m 值越大, 要求联合解码的节点数就越多, 即解码的成功率越低, 系统的保密性越强.

推论 1 ACM-NC 中除信宿节点外, 其他任何节点均无法还原信源节点的原始通信消息.

证明 发送匿名组中通信消息的嵌套加密机制有效阻止恶意节点的窃听和流量分析等攻击行为, 即使通信链路中某个节点被攻击者所控制, 由于该节点仅掌握自己的会话密钥, 则攻击者仅能获知该节点的直接前驱和直接后继的相关信息, 根本无法获知信源节点的原始通信消息. 接收匿名组中除信宿节点外的其他成员, 无法获知准确的信宿节点身份信息而无法还原信源节点的原始通信消息. 由定理 3 和定理 4 可知, 编码匿名转发网络中任意节点均无法还原信源节点的原始通信消息. 因而在 ACM-NC 中除信宿节点外, 其他任何节点均无法还原信源节点的原始通信消息.

推论 2 当编码匿名转发网络中任意 X ($X \leq 0.7mn$) 个恶意节点进行合谋解码时, 恶意节点依然很难获知信源节点的原始通信消息, 即编码匿名转发网络具有较强的匿名性和安全性.

证明 由定理 4 可知推论 2 成立.

4.4 技术对比

AC-ITNC^[5] 和传统匿名通信系统均由密钥协商和匿名通信两个阶段组成, 并基于密钥建立匿名通信链路, 匿名链路的首节点可获知信源节点的位置信息, 而链路的尾节点可获知信宿节点的位置信息; 匿名通信过程的安全性基于密钥的安全性构建; 在通信过程中使用了消息填充机制, 导致系统的通信时延较大; 由于 AC-ITNC 无需可信的密钥管理中心, 因而其推广性较好, 传统匿名通信系统中需要可信的密钥管理中心进行密钥的管理, 推广性较差.

本文 ACM-NC 无需密钥协商, 采用编码技术构建匿名通信路径, 并且无需可信的密钥管理中心, 具有较好的推广性; 同时, 匿名链路中的任意节点都无法获知信源及信宿节点的位置信息, 很好的保护了信源节点和信宿节点的匿名性, 并且在通信过程中无需进行消息填充, 而采用编码技术实现通信消息的匿名性.

4.5 复杂度分析

(1) 时间复杂度

在 ACM-NC 中, 因 $L_S > m$, 所以信源节点匿名通信消息伪装算法和发送匿名链路中节点 $\text{Node}_{(i)}$ 消息转发策略的时间复杂度都为 $O(L_S)$; 转发网络中节点 $O_{(i,j)} (i=1, 2, \dots, m, j=1, 2, \dots, n-1)$ 编码转发算法的时间复杂度为 $O(m)$, 节点 $O_{(i,n)}$ 的时间复杂度为 $O(L_R)$, 则编码匿名转发网络的时间复杂度为 $m(n-1)O(m) + mO(L_R)$.

通常 ACM-NC 中 $m(m=4)$ 和 $n(n=3)$ 均为确定的值, 因此 ACM-NC 的时间复杂度为级别较小的线性复杂度.

(2) 空间复杂度

编码匿名转发网络中各节点需要存储空间用于存放路由表, 因而节点 $O_{(i,j)}$ 的空间复杂度为 $O(m)$, 节点 $O_{(i,n)}$ 的空间复杂度为 $O(L_R)$, 则编码匿名转发网络的空间复杂度为 $m(n-1)O(m) + mO(L_R)$.

通常 ACM-NC 中 $m(m=4)$ 和 $n(n=3)$ 均为确定的值, 因此 ACM-NC 的空间复杂度为级别较低的线性复杂度.

5 结论

本文基于信息分割理论和网络编码技术, 提出基于网络编码的匿名通信模型 ACM-NC, 通过编码匿名转发网络的消息编码增加攻击者对窃听信息进行数据包分析的难度, 保证了通信消息传输的不可追踪性和抗合谋攻击能力, 显著提高了 ACM-NC 的匿名性、安全性和保密性. 在无信任中心的网络环境下, 通过信源节点和编码匿名转发网络对通信消息的编码操作, 有效地实现通信消息传输的匿名性, 不仅提供信源节点和信宿节点的匿名性以及通信消息的保密性, 也克服了传统的匿名通信方法中以提高方案复杂度来换取匿名性的局限性. 本文 ACM-NC 将信息分割策略和网络编码技术应用于匿名通信阶段, 为编码混淆匿名通信模型的研究提供了理论依据.

本文 ACM-NC 是在假设网络不出现差错的环境中进行编码信息的解码研究, 未来将研究 ACM-NC 的容错方法及技术, 以保证网络编码的正确性和有效性, 进一步优化 ACM-NC.

参考文献

- 1 Goldschlag D, Reed M, Syverson P. Onion routing for anonymous and private internet connections. *Commun ACM*, 1999, 42: 39–41
- 2 Dingledine R, Mathewson N, Syverson P. Tor: the second-generation onion router. In: *Proceedings of the 13th USENIX Security Symposium*, Berkeley, 2004. 303–320
- 3 Chaum D L. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun ACM*, 1981, 24: 84–88
- 4 Reiter M K, Rubin A D. Crowds: anonymity for web transactions. *ACM Trans Inform Syst Sec*, 1998, 1: 66–92
- 5 Duan G H, Wang W P, Wang J X, et al. Anonymous communication mechanism with multi-paths network coding. *J Softw*, 2010, 21: 2338–2351 [段桂华, 王伟平, 王建新, 等. 一种基于多路径网络编码的匿名通信机制. *软件学报*, 2010, 21: 2338–2351]

- 6 Chaum D. The dining cryptographers problem: unconditional sender and recipient untraceability. *J Cryptol*, 1988, 1: 65–75
- 7 Sherwood R, Bhattacharjee B, Srinivasan A. P5: a protocol for scalable anonymous communication. *J Comput Sec*, 2005, 13: 839–876
- 8 Freedman M J, Morris R. Tarzan: a peer-to-peer anonymizing network layer. In: *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002)*, Washington, 2002. 193–206
- 9 Katti S, Katabi D, Puchala K. Slicing the Onion: Anonymous Routing Without PKI. Technical Report. MIT-CSAIL-TR-2005-053, Cambridge: Massachusetts Institute of Technology, 2005
- 10 Katti S, Cohen J, Katabi D. Information slicing: anonymity using unreliable overlays. In: *Proceedings of the 4th USENIX Symposium on Network Systems Design and Implementation*, Berkeley, 2007. 43–56
- 11 Ahlswede R, Cai N, Li S Y, et al. Network information flow. *IEEE Trans Inform Theory*, 2000, 46: 1204–1216
- 12 Li S Y R, Yeung R W. Linear network coding. *IEEE Trans Inform Theory*, 2000
- 13 Ho T, Karger D, Medard M, et al. The benefits of coding over routing in a randomized setting. *IEEE Int Symp Inform Theory*, 2003
- 14 Koeter R, Medard M. An algebraic approach to network coding. *IEEE/ACM Trans Netw*, 2003, 11: 782–795
- 15 Sanders P, Egner S, Tolhuizen L. Polynomial time algorithms for network information flow. In: *Proceedings of 15th ACM Symposium on Parallel Algorithms and Architectures*, New York, 2003. 286–294
- 16 Wang J, Wang J P, Wu C, et al. Anonymous communication with network coding against traffic analysis attack. In: *Proceedings of INFOCOM*, Shanghai, 2011. 1008–1016
- 17 Jaggi S, Chou P A, Jain K. Low complexity algebraic network codes. In: *Proceedings of the IEEE International Symposium on Information Theory*, 2003
- 18 Fragouli C, Soljanin E. Information flow decomposition for network coding. *IEEE Trans Inform Theory*, 2006, 52: 829–848
- 19 Chou P A, Wu Y, Jain K. Practical network coding. In: *Proceedings of the 41th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, 2003. 40–49
- 20 Zhao Y. Research on the Key Wireless Transmission Technologies Based on Network Coding. Ph. D. Dissertation. Beijing: Beijing University of Posts and Telecommunications, 2012 [赵渊. 基于网络编码的无线传输关键技术研究. 博士学位论文. 北京邮电大学, 2012]
- 21 Deb S, Effros M, Ho T, et al. Network coding for wireless applications: a brief tutorial. In: *Proceedings of IWWMAN*, London, 2005
- 22 Al Hamra A, Barakat C, Turetli T. Network coding for wireless mesh networks: a case study. In: *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, Niagara-Falls, Buffalo-NY, 2006. 103–114
- 23 Wu Y N, Kung S Y. Reduced-complexity network coding for multicasting over ad-hoc networks. In: *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2005. 501–504
- 24 Hou H F, Ji X S, Liu G Q. Identity-based anonymity authentication protocol in the heterogeneous wireless network. *J Commun*, 2011, 32: 153–161 [侯惠芳, 季新生, 刘光强. 异构无线网络中基于标识的匿名认证协议. 通信学报, 2011, 32: 153–161]
- 25 Wu Z Q, Zhou Y W, Ma J F. A security transmission model for internet of things. *Chin J Comput*, 2011, 34: 1351–1364 [吴振强, 周彦伟, 马建峰. 物联网安全传输模型. 计算机学报, 2011, 34: 1351–1364]
- 26 Wu Z Q, Zhou Y W, Qiao Z R. Access mechanism of TMP under mobile network. *J Commun*, 2010, 31: 158–169 [吴振强, 周彦伟, 乔子芮. 移动互联网下可信移动平台接入机制. 通信学报, 2010, 31: 158–169]

Anonymous communication model based on network coding

ZHOU YanWei^{1,2}, YANG Bo^{2*}, WU ZhenQiang^{1,2}, HE JuHou^{1,2} & LI Jun¹

1 Key Laboratory of Modern Teaching Technology, Ministry of Education, Xi'an 710062, China;

2 School of Computer Science, Shaanxi Normal University, Xi'an 710062, China

*E-mail: byang@snnu.edu.cn

Abstract The transmission mode of traditional network has been significantly changed by the network coding technology. This paper proposed a new anonymous communication model based on information slicing theory and network coding technology, which is ACM-NC (anonymous communication model based on network coding). As to this ACM-NC, the messages are transmitted through different anonymous links after being sliced by information slicing technology, which could effectively improve the anonymity, security and confidentiality of this model as well as enhance its ability of against conspiracy attack. The analysis approves that the ACM-NC has strong anonymity, security and confidentiality, and only the destination node can decode and restore the original anonymous communication messages, which is encoded and sent from the source node.

Keywords information slicing, anonymous communication, network coding, conspiracy attack, network security

ZHOU YanWei was born in 1986. He received the B.S. and M.S. degree in computer science and computer systems organization from Shaanxi Normal University in 2008 and 2011 respectively. His research interests include anonymous communication, wireless communication and cryptography. He currently focuses on provably secure two-party certificateless key agreement protocol.

YANG Bo was born in 1963. He received the Ph.D. degree in cryptography from Xidian University, Xi'an, in 1999. His research interests include information security and cryptography. He has been currently a professor in the school of computer science at the Shaanxi Normal University. He is a director of CACR, and is a member of CCF.

WU ZhenQiang was born in 1968. He received the Ph.D. degree in cryptography from Xidian University, Xi'an, in 2007. His research interests include anonymous communication, trusted computing, pervasive computing and network coding. He has been currently a professor in the school of computer science at the Shaanxi Normal University. He is a member of CCF.

HE JuHou was born in 1972. He received the Ph.D. degree in computer application from Northwestern Polytechnical University, Xi'an, in 2005. His research interests include information security and educational technology. He is currently an associate professor in the Key Laboratory of Modern Teaching Technology at the Shaanxi Normal University. He is a member of CCF.